Amendments to the Drawings

Proposed replacement drawings are submitted herewith for Figs. 4B and 4C (which are now split into Figs. 4B1 and 4B2, 4C1 and 4C2), 6, 7C, 8A, 9B, 10A - 10C, and 12 to correct problems with margins in accordance with the Draftsperson's review.

In addition, the notation

DN="cn=doctors,ou=groups,o=acme"

is replaced with the notation

DN="cn=medical,ou=groups,o=acme"

in Figs. 4B1 and 4C1. That is, "doctors" is replaced with "medical". This aligns the terminology in the figures with the text on Page 51, line 1 of the specification as originally filed.

No new matter is introduced with these proposed replacement drawings, all of which are supported by the specification and drawings as originally filed.

PAGE 63/89 * RCVD AT 4/7/2004 6:57:11 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:8729306 * CSID:4073437587 * DURATION (mm-ss):21-30

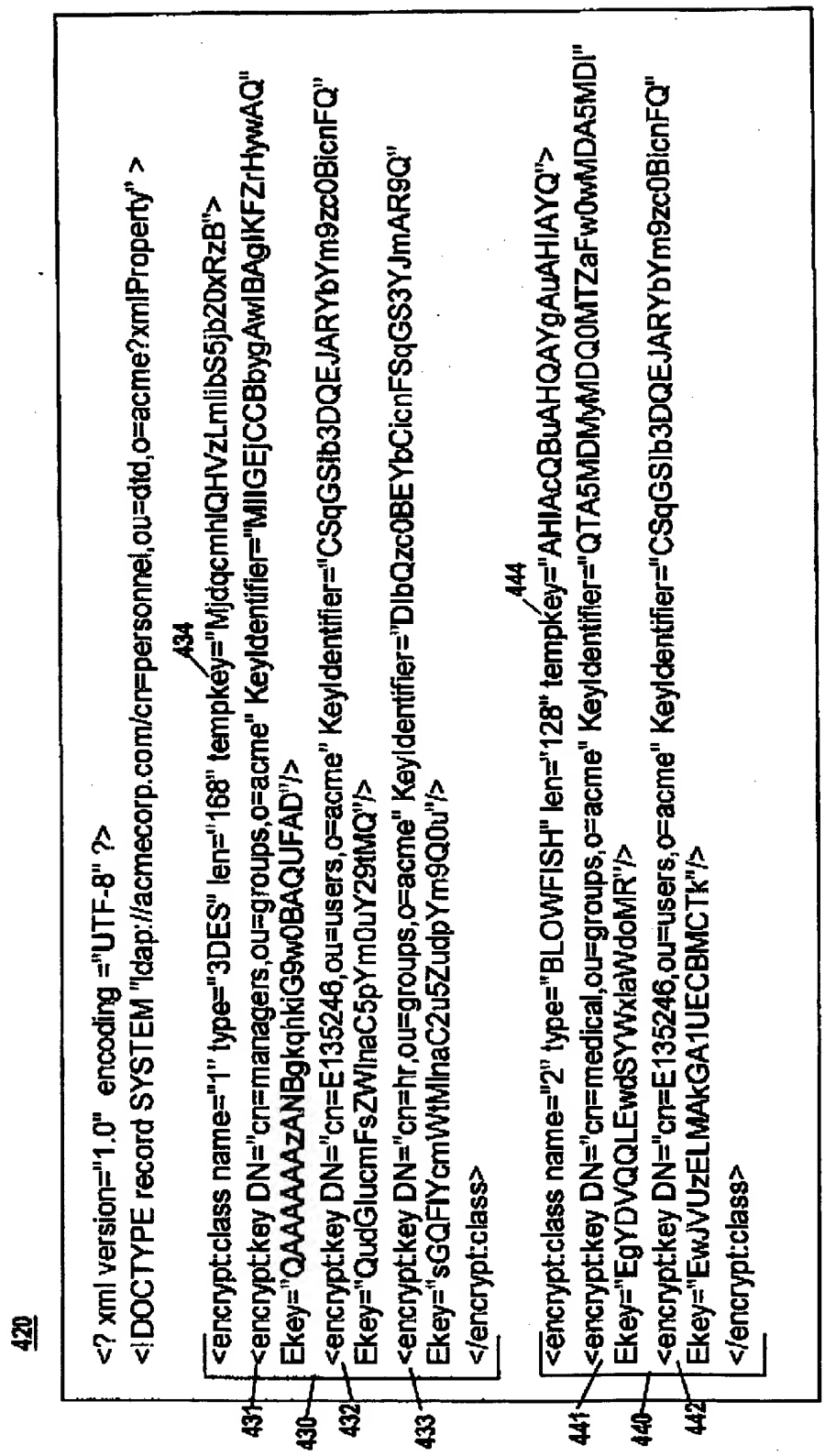

420
<? xml version="1.0" encoding ="UTF-8" ?>
<!DOCTYPE record SYSTEM "ldap://acmecorp.com/cn=personnel,ou=dtd,o=acme?xmlProperty" >
<encrypt:class name="1" type="3DES" len="168" tempkey="MjdqcmhlQHVzLmlibS5jb20xRzB">
434
<encrypt:key DN="cn=managers,ou=groups,o=acme" KeyIdentifier="MIIGEjCCBbygAwIBAgIKFZrHywAQ"
Ekey="QAAAAAAzANBgkqhkiG9w0BAQUFAD"/>
<encrypt:key DN="cn=E135246,ou=users,o=acme" KeyIdentifier="CSqGSIb3DQEJARYbYm9zc0BicnFQ"
Ekey="QudGlucmFsZWlnaC5pYm0uY29tMQ"/>
<encrypt:key DN="cn=hr,ou=groups,o=acme" KeyIdentifier="DlbQzc0BEYbCicnFSqGS3YJmAR9Q"
Ekey="sGQFIYcmWtMlnaC2u5ZudpYm9Q0u"/>
</encrypt:class>
444
<encrypt:class name="2" type="BLOWFISH" len="128" tempkey="AHIAcQBuAHQAYgAuAHIAYQ">
<encrypt:key DN="cn=medical,ou=groups,o=acme" KeyIdentifier="QTA5MDMyMDQ0MTZaFw0wMDA5MDI"
Ekey="EgYDVQQLEwdSYWxlaWdoMR"/>
<encrypt:key DN="cn=E135246,ou=users,o=acme" KeyIdentifier="CSqGSIb3DQEJARYbYm9zc0BicnFQ"
Ekey="EwJVUzELMAkGA1UECBMCTk"/>
</encrypt:class>
431
430
432
433
441
440
442

Fig. 4B1

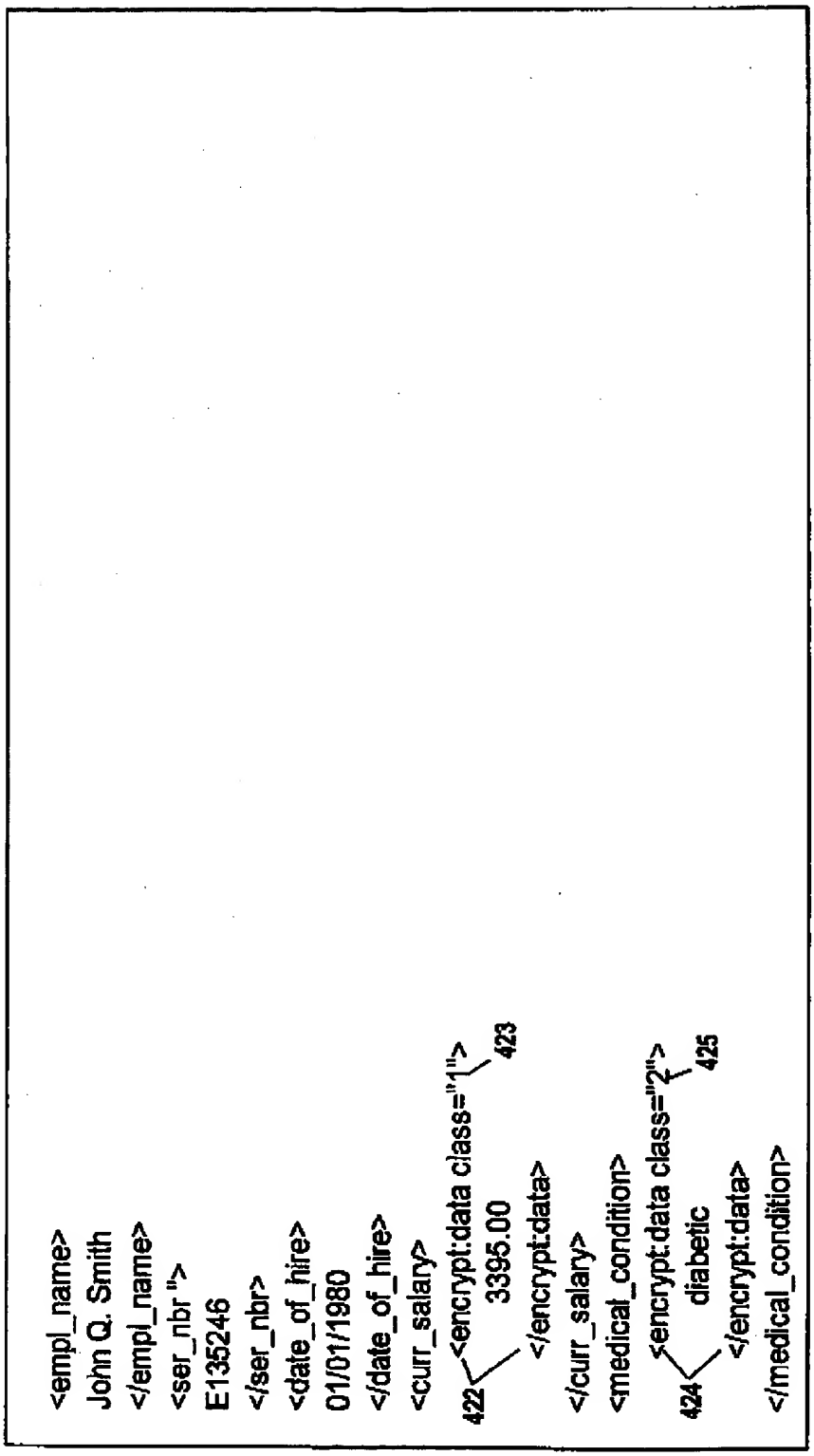

420 (cont'd)
<empl_name>
John Q. Smith
</empl_name>
<ser_nbr ">
E135246
</ser_nbr>
<date_of_hire>
01/01/1980
</date_of_hire>
<curr_salary>
<encrypt:data class="1">
422
423
3395.00
</encrypt:data>
</curr_salary>
<medical_condition>
<encrypt:data class="2">
424
425
diabetic
</encrypt:data>
</medical_condition>

Fig. 4B2

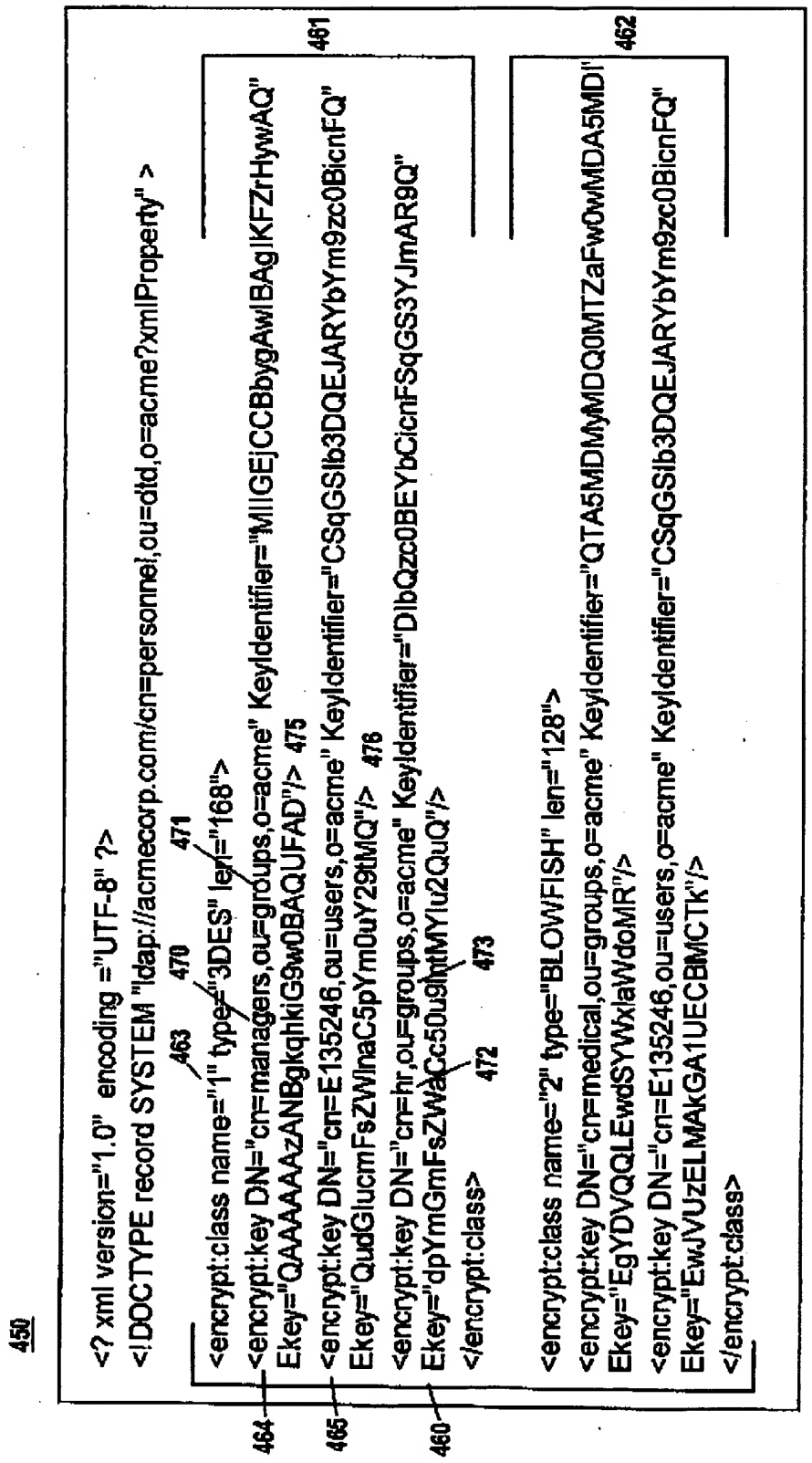

450
<? xml version="1.0" encoding ="UTF-8" ?>
<!DOCTYPE record SYSTEM "ldap://acmecorp.com/cn=personnel,ou=dtd,o=acme?xmlProperty" >
463
470
471
<encrypt:class name="1" type="3DES" len="168">
<encrypt:key DN="cn=managers,ou=groups,o=acme" KeyIdentifier="MIIGEjCCBbygAwIBAgIKFZrHywAQ"
Ekey="QAAAAAAzANBgkqhkiG9w0BAQUFAD"/> 475
<encrypt:key DN="cn=E135246,ou=users,o=acme" KeyIdentifier="CSqGSIb3DQEJARYbYm9zc0BicnFQ"
Ekey="QudGlucmFsZWlnaC5pYm0uY29tMQ"/> 476
<encrypt:key DN="cn=hr,ou=groups,o=acme" KeyIdentifier="DlbQzc0BEYbCicnFSqGS3YJmAR9Q"
Ekey="dpYmGmFsZWlaCc50u9hqtMYlu2QuQ"/>
</encrypt:class>
472
473
461
<encrypt:class name="2" type="BLOWFISH" len="128">
<encrypt:key DN="cn=medical,ou=groups,o=acme" KeyIdentifier="QTA5MDMyMDQ0MTZaFw0wMDA5MD
Ekey="EgYDVQQLEwdSYWxlaWdoMR"/>
<encrypt:key DN="cn=E135246,ou=users,o=acme" KeyIdentifier="CSqGSIb3DQEJARYbYm9zc0BicnFQ"
Ekey="EwJVUzELMAkGA1UECBMCTk"/>
</encrypt:class>
462
464
465
460

Fig. 4C1

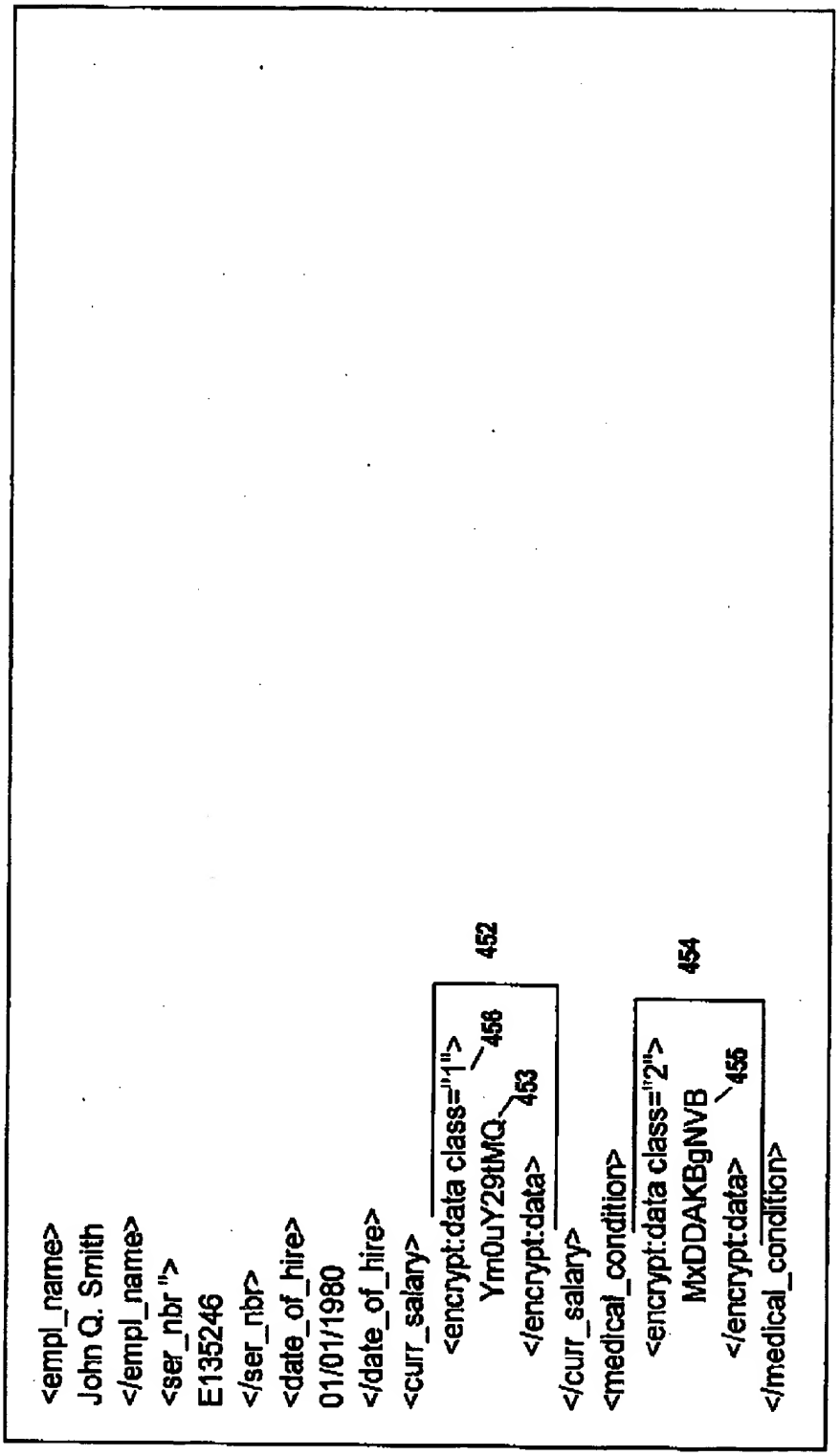

450 (cont'd)
<empl_name>
John Q. Smith
</empl_name>
<ser_nbr ">
E135246
</ser_nbr>
<date_of_hire>
01/01/1980
</date_of_hire>
<curr_salary>
<encrypt:data class="1">
Ym0uY29tMQ
</encrypt:data>
</curr_salary>
<medical_condition>
<encrypt:data class="2">
MxDDAKBgNVB
</encrypt:data>
</medical_condition>
452
453
454
455
456

Fig. 4C2

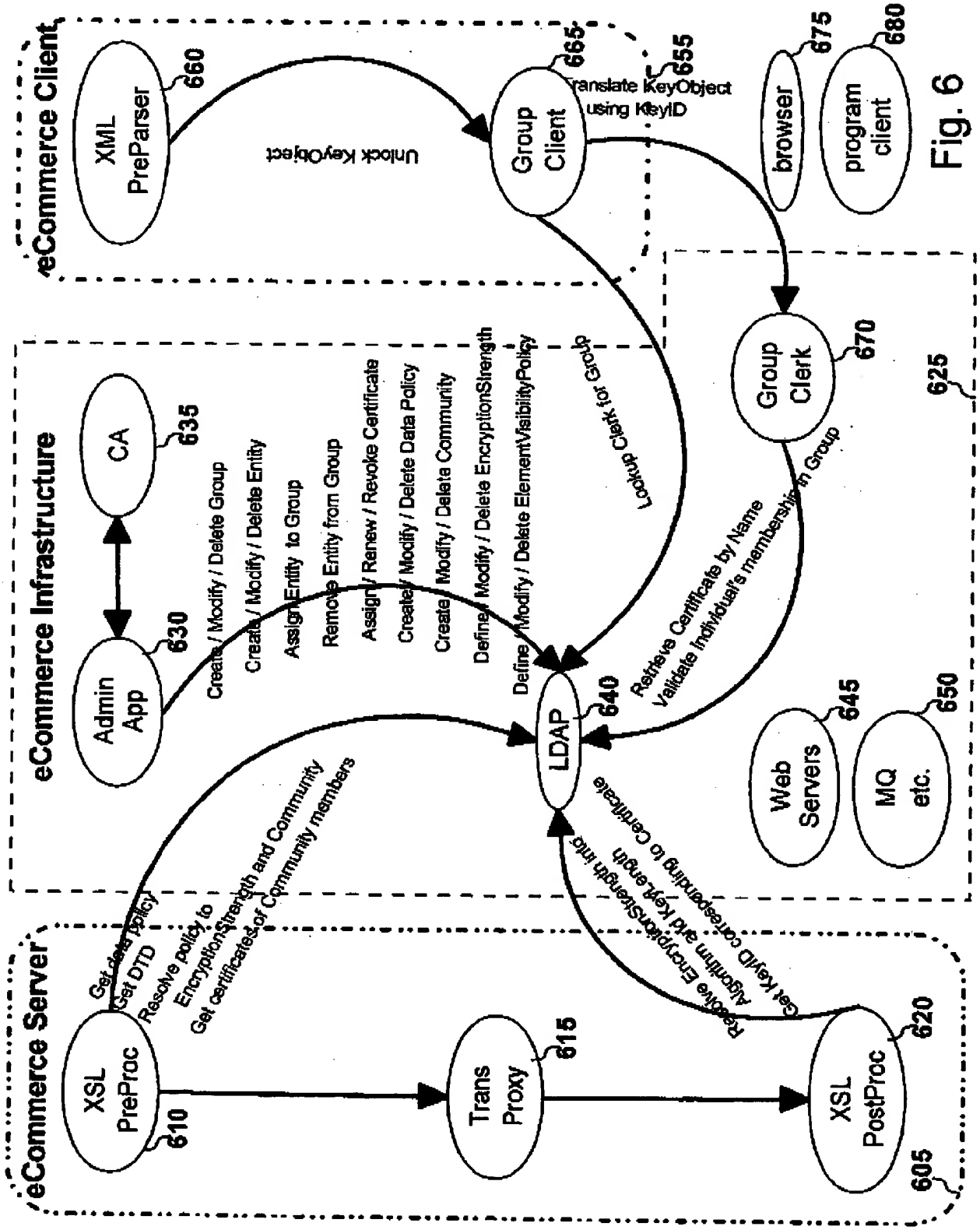

eCommerce Client
XML PreParser
660
Unlock KeyObject
Group Client
665
Translate KeyObject using KeyID
655
browser
675
program client
680
eCommerce Infrastructure
CA
635
Admin App
630
Create / Modify / Delete Group
Create / Modify / Delete Entity
Assign Entity to Group
Remove Entity from Group
Assign / Renew / Revoke Certificate
Create / Modify / Delete Data Policy
Create / Modify / Delete Community
Define / Modify / Delete EncryptionStrength
Define / Modify / Delete ElementVisibilityPolicy
Lookup Clerk for Group
Group Clerk
670
625
Retrieve Certificate by Name
Validate Individual's membership in Group
LDAP
640
Web Servers
645
MQ etc.
650
eCommerce Server
Get data policy
Get DTD
Resolve policy to EncryptionStrength and Community
Get certificates of Community members
Resolve EncryptionStrength into Algorithm and KeyLength
Get KeyID corresponding to Certificate
XSL PreProc
610
Trans Proxy
615
XSL PostProc
620
605

Fig. 6

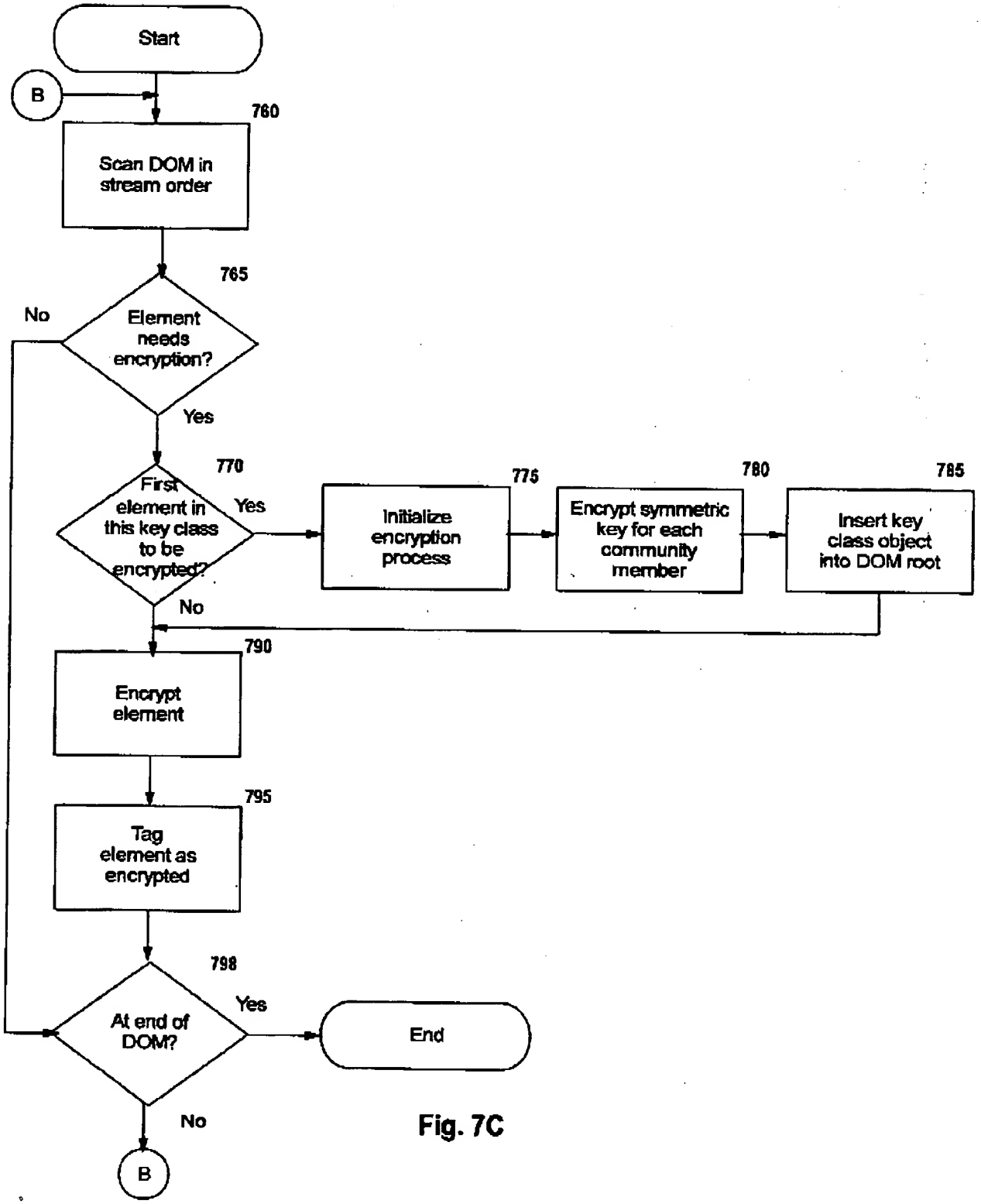

Start
B
760
Scan DOM in stream order
765
Element needs encryption?
No
Yes
770
First element in this key class to be encrypted?
Yes
775
Initialize encryption process
780
Encrypt symmetric key for each community member
785
Insert key class object into DOM root
No
790
Encrypt element
795
Tag element as encrypted
798
At end of DOM?
Yes
End
No
B

Fig. 7C

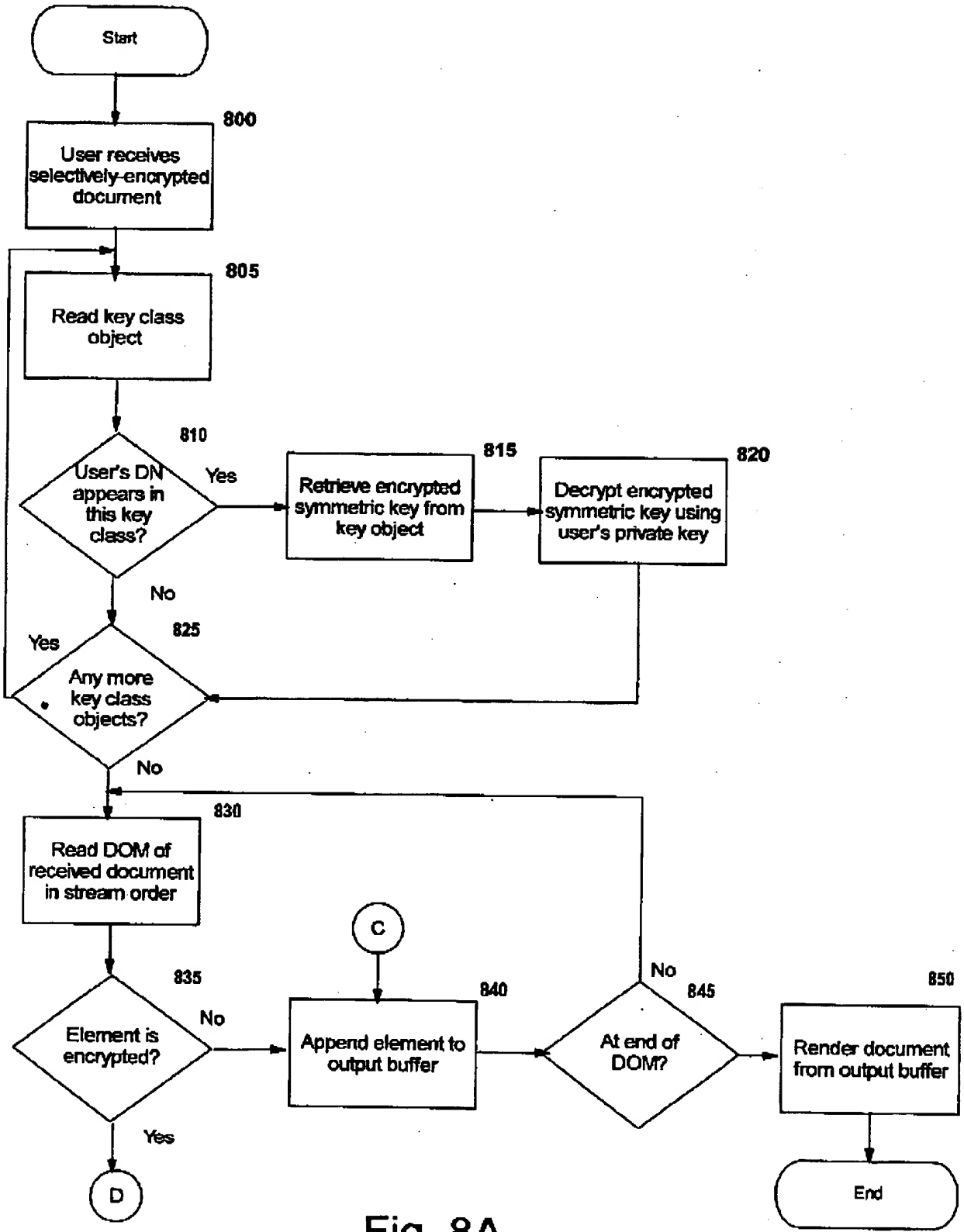

Start
800
User receives selectively-encrypted document
805
Read key class object
810
User's DN appears in this key class?
Yes
815
Retrieve encrypted symmetric key from key object
820
Decrypt encrypted symmetric key using user's private key
No
Yes
825
Any more key class objects?
No
830
Read DOM of received document in stream order
C
835
Element is encrypted?
No
840
Append element to output buffer
No
845
At end of DOM?
850
Render document from output buffer
Yes
D
End

Fig. 8A

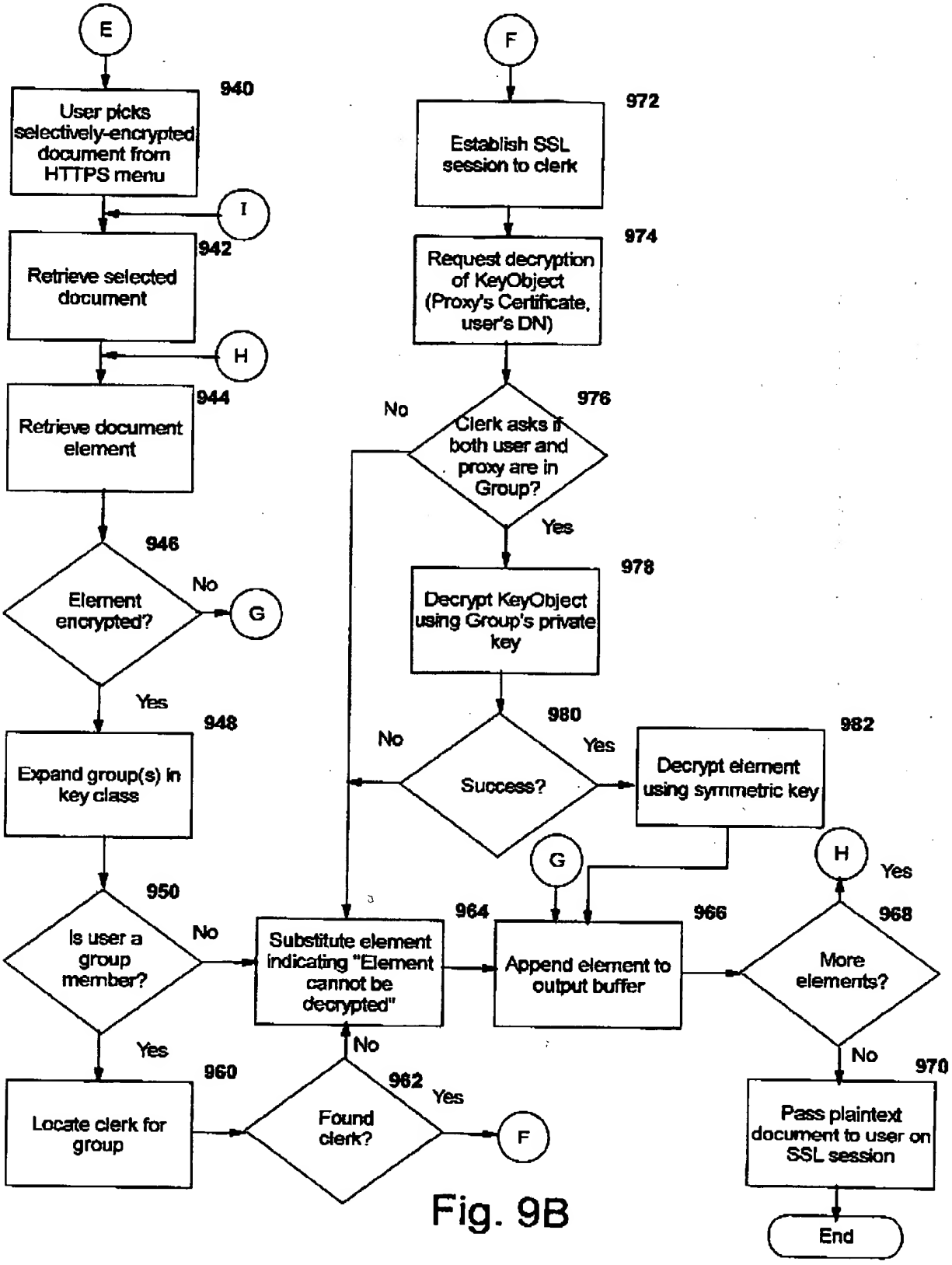

E
User picks selectively-encrypted document from HTTPS menu
940
I
Retrieve selected document
942
H
Retrieve document element
944
Element encrypted?
946
No
G
Yes
Expand group(s) in key class
948
Is user a group member?
950
No
Yes
Locate clerk for group
960
Found clerk?
962
No
Yes
F
Substitute element indicating "Element cannot be decrypted"
964
Append element to output buffer
966
More elements?
968
Yes
No
Pass plaintext document to user on SSL session
970
End
F
Establish SSL session to clerk
972
Request decryption of KeyObject (Proxy's Certificate, user's DN)
974
Clerk asks if both user and proxy are in Group?
976
No
Yes
Decrypt KeyObject using Group's private key
978
Success?
980
No
Yes
Decrypt element using symmetric key
982
G
H

Fig. 9B

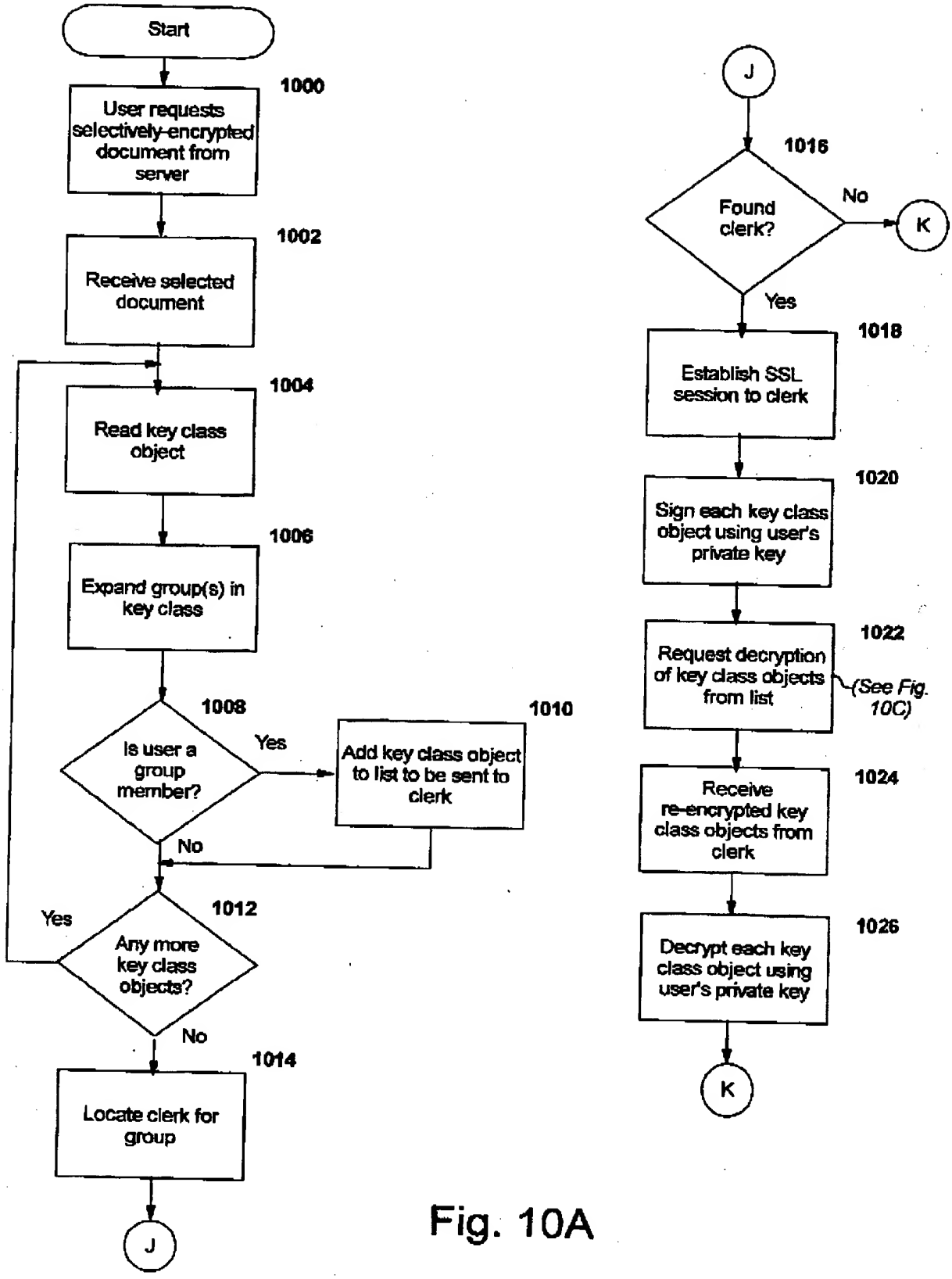

Start
1000
User requests selectively-encrypted document from server
1002
Receive selected document
1004
Read key class object
1006
Expand group(s) in key class
1008
Is user a group member?
Yes
1010
Add key class object to list to be sent to clerk
No
1012
Any more key class objects?
Yes
No
1014
Locate clerk for group
J
J
1016
Found clerk?
No
K
Yes
1018
Establish SSL session to clerk
1020
Sign each key class object using user's private key
1022
Request decryption of key class objects from list
(See Fig. 10C)
1024
Receive re-encrypted key class objects from clerk
1026
Decrypt each key class object using user's private key
K

Fig. 10A

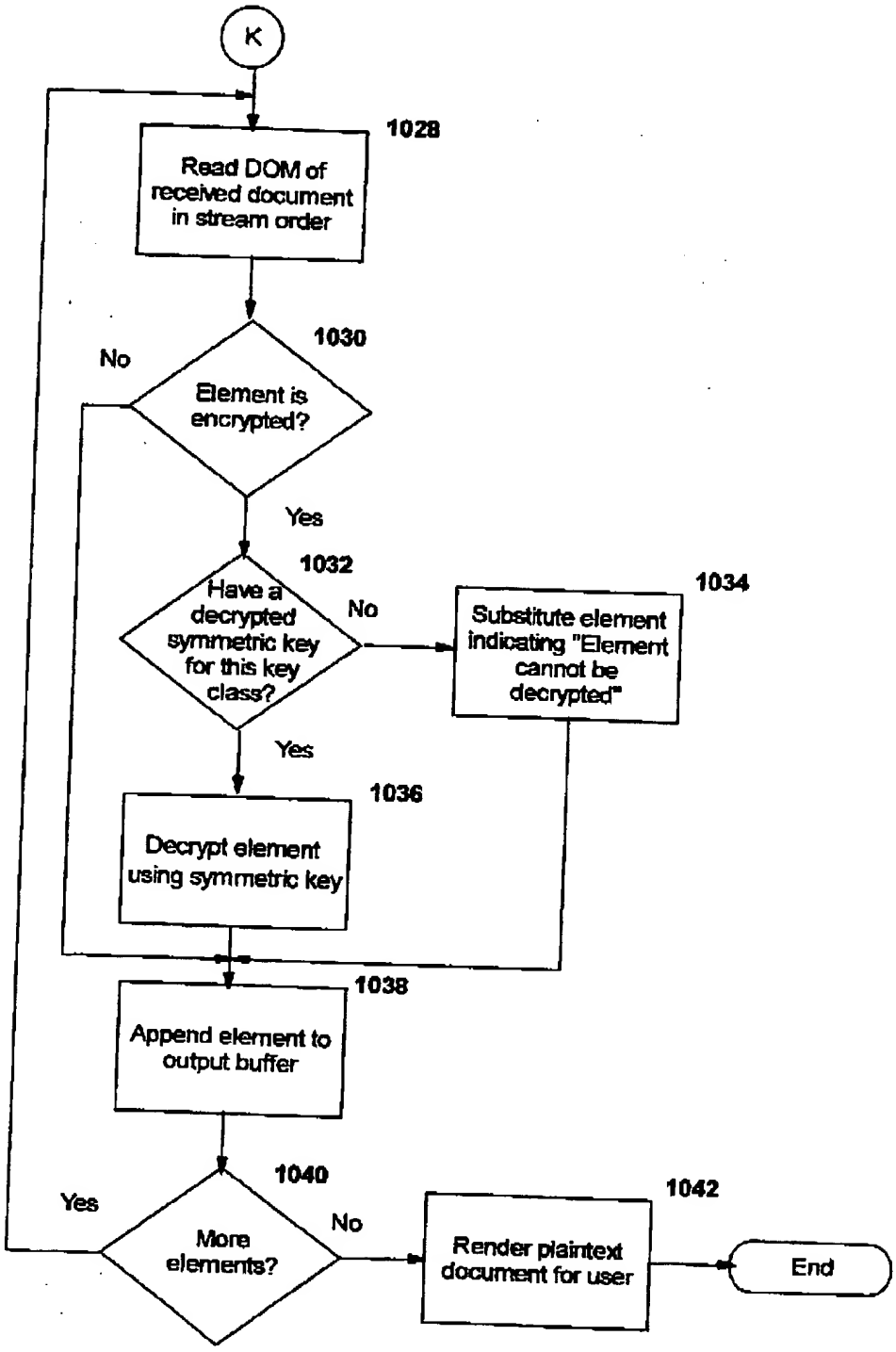

K
1028
Read DOM of received document in stream order
1030
No
Element is encrypted?
Yes
1032
Have a decrypted symmetric key for this key class?
No
1034
Substitute element indicating "Element cannot be decrypted"
Yes
1036
Decrypt element using symmetric key
1038
Append element to output buffer
1040
Yes
More elements?
No
1042
Render plaintext document for user
End

Fig. 10B

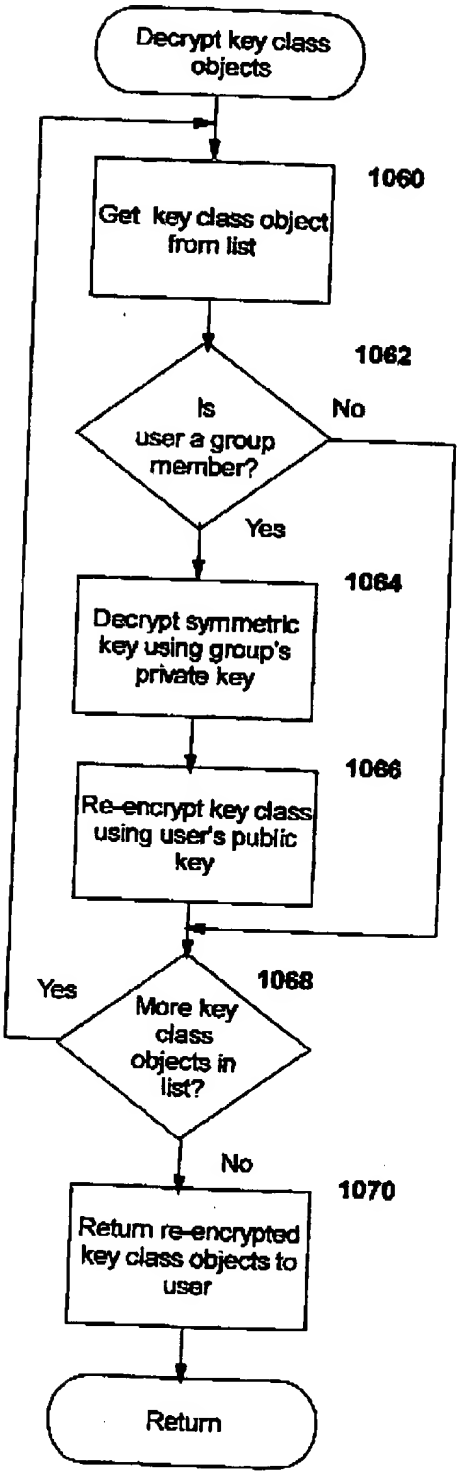
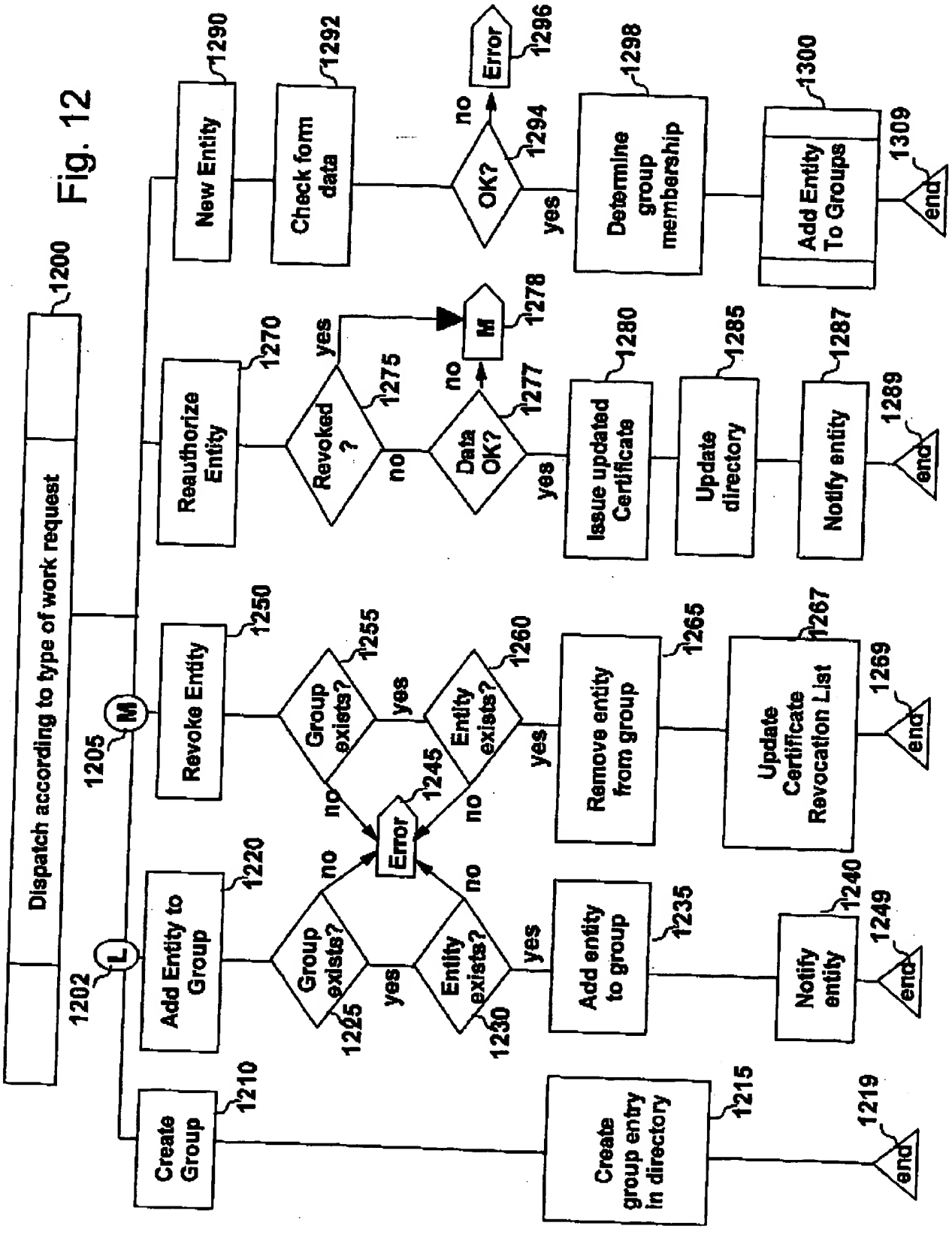

Decrypt key class objects
1060
Get key class object from list
1062
Is user a group member?
No
Yes
1064
Decrypt symmetric key using group's private key
1066
Re-encrypt key class using user's public key
1068
Yes
More key class objects in list?
No
1070
Return re-encrypted key class objects to user
Return

Fig. 10C

Fig. 12


Dispatch according to type of work request
1200
1202
1205
M
L
New Entity
1290
Check form data
1292
Error
1296
no
OK?
1294
yes
Determine group membership
1298
Add Entity To Groups
1300
1309
end
Reauthorize Entity
1270
Revoked ?
1275
yes
no
M
1278
Data OK?
1277
no
yes
Issue updated Certificate
1280
Update directory
1285
Notify entity
1287
1289
end
Revoke Entity
1250
Group exists?
1255
yes
no
Entity exists?
1260
yes
no
Error
1245
Remove entity from group
1265
Update Certificate Revocation List
1267
1269
end
Add Entity to Group
1220
Group exists?
1225
yes
no
Entity exists?
1230
yes
no
Add entity to group
1235
Notify entity
1240
1249
end
Create Group
1210
Create group entry in directory
1215
1219
end